INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-22 14:02 UTC

ClickOnce Framework Abused for Privilegeless Persistence via .appref-ms, dfsvc.exe, and rundll32.exe

THREAT CAMPAIGN | **HIGH** | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0536
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	5.0
Affected Products	Microsoft Windows, ClickOnce deployment framework (.appref-ms files, dfsvc.exe, rundll32.exe process chains); all standard Windows endpoints where ClickOnce is enabled
Discovery Source	Rss:T1 Threatintel

Executive Summary

Researchers at CrowdStrike have documented active abuse of Microsoft's ClickOnce deployment framework, a legitimate Windows technology, to achieve persistent footholds on endpoints without requiring administrator privileges. Attackers deliver malicious .appref-ms files, commonly via email, then leverage Windows-native processes (dfsvc.exe, rundll32.exe) to install payloads and maintain silent, self-updating persistence that bypasses many standard email and endpoint controls. Any organization running standard Windows endpoints is exposed; the attack requires no elevated rights and exploits trusted Microsoft infrastructure, making detection and containment non-trivial because the technique relies entirely on legitimate Microsoft processes and infrastructure.

Technical Analysis

This campaign exploits Microsoft's ClickOnce deployment framework across standard Windows endpoints where ClickOnce is enabled by default. The attack chain uses three primary components: .appref-ms file associations (application reference files that trigger ClickOnce installations), dfsvc.exe (the ClickOnce deployment service host), and rundll32.exe process trees spawned during installation. Because standard Windows user accounts can install ClickOnce applications without elevation, attackers achieve privilegeless persistence, a bypass of privilege escalation and software installation controls. The framework's legitimate update mechanism enables silent remote payload swaps via attacker-controlled update servers, complicating eradication. .application and .appref-ms files frequently bypass email gateway filters tuned for .exe and Office macro scrutiny. No CVE has been assigned to this technique; it exploits intended ClickOnce behavior rather

than a patched vulnerability. Relevant CWEs: CWE-494 (Download of Code Without Integrity Check) and CWE-693 (Protection Mechanism Failure). MITRE ATT&CK coverage includes T1566.002 (Spearphishing Link), T1218/T1218.011 (Signed Binary Proxy Execution via rundll32.exe), T1547/T1547.001 (Boot/Logon Autostart, Registry Run Keys), T1105 (Ingress Tool Transfer), T1053.005 (Scheduled Task), T1027 (Obfuscated Files), T1574 (Hijack Execution Flow), and T1204.002 (Malicious File execution). Source: CrowdStrike blog series, Parts 1 and 2.

Action Checklist

1. Step 1: Containment, Audit email gateway rules immediately and add explicit block or quarantine policies for .appref-ms and .application file attachments and download links. Confirm web proxy or secure email gateway inspects ClickOnce MIME types (application/x-ms-application, application/x-ms-appref-ms). Identify any .appref-ms files delivered to mailboxes in the past 90 days using email search tools.
2. Step 2: Detection, Query endpoint telemetry for dfsvc.exe spawning child processes (cmd.exe, powershell.exe, rundll32.exe, wscript.exe), this process tree is anomalous outside legitimate enterprise ClickOnce deployments. Search Windows event logs and EDR for .appref-ms file execution (process creation events showing dfsvc.exe as parent). Review HKCU\Software\Microsoft\Windows\CurrentVersion\Run and user-writable startup locations for ClickOnce-registered application shortcuts. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS Controls v8 Audit Logging to validate log coverage across endpoints.
3. Step 3: Eradication, There is no vendor patch; this technique exploits intended ClickOnce behavior. Where ClickOnce is not required for business operations, disable the feature via Group Policy (Software Restriction Policies or AppLocker rules blocking dfsvc.exe execution for standard users). Remove any identified malicious .appref-ms shortcuts from user profiles and startup locations. Revoke or rotate credentials for accounts that executed suspicious ClickOnce payloads per NIST AC-2 (Account Management) and credential rotation procedures.
4. Step 4: Recovery, After disabling or restricting ClickOnce, validate that legitimate business-critical ClickOnce applications are inventoried and explicitly allowlisted before re-enabling selectively. Monitor dfsvc.exe process activity for 30 days post-remediation. Confirm no persistent scheduled tasks or Run key entries tied to attacker-controlled update URLs remain. Apply NIST AU-12 (Audit Record Generation) controls to ensure post-remediation activity is fully logged.
5. Step 5: Post-Incident, Conduct a gap review of email gateway rules against non-.exe delivery mechanisms (.appref-ms, .application, .lnk, .hta, .iso). Map detection coverage against T1218 (Signed Binary Proxy Execution) and T1547.001 (Registry Run Keys) in your SIEM or EDR. Reference CIS 7.1 (Vulnerability Management Process) to formalize periodic review of LOLBin and living-off-the-land technique coverage. Engage threat hunting to baseline dfsvc.exe activity across the estate using system file analysis and local account monitoring to identify residual indicators.

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate immediately to senior IR leadership and legal/compliance if dfsvc.exe child process chains or attacker-controlled ClickOnce update URLs are confirmed on hosts processing PII, PHI, or financial data, as credential harvesting payloads delivered via this campaign may trigger breach notification obligations under HIPAA, GDPR, or PCI-DSS; also escalate if the technique is detected on more than 5% of the endpoint estate or on any privileged administrator workstation, indicating active lateral movement beyond initial ClickOnce delivery.
Recovery Notes	Before restoring full endpoint operation, validate that all %LOCALAPPDATA%\Apps\2.0\ directories on remediated hosts contain only manifests signed by known-good publishers and that no outbound connections to the attacker's ClickOnce distribution infrastructure (identified from the 'deploymentProvider' URL in recovered manifests) appear in proxy logs. Monitor dfsvc.exe process creation events via Sysmon Event ID 1 continuously for a minimum of 30 days post-remediation, as ClickOnce's built-in auto-update mechanism may re-execute a payload if the attacker's distribution URL was not fully blocked at the network perimeter. Re-baseline the HKCU Run key and Startup folder contents on all remediated user profiles at day 7 and day 30 to confirm no re-registration of ClickOnce persistence entries has occurred.
Forensic Artifacts	%LOCALAPPDATA%\Apps\2.0\ directory tree — ClickOnce installs all user-level applications here without admin rights; malicious payloads, deployment manifests (.application XML), and the attacker's update URL ('deploymentProvider' element) are stored in randomized subdirectories under this path and will survive reboots until explicitly removed | Sysmon Event ID 1 (Process Create) logs filtered on ParentImage=dfsvc.exe — records the full command line of cmd.exe, powershell.exe, rundll32.exe, or wscript.exe spawned by the ClickOnce deployment service, which is the primary behavioral indicator of malicious payload execution in this campaign | Windows Security Event ID 4688 (Process Creation) with creator process name dfsvc.exe and Windows Security Event ID 4698 (Scheduled Task Created) — documents both the initial execution chain and any attacker-registered scheduled tasks used as a secondary persistence mechanism alongside the HKCU Run key | HKCU\Software\Microsoft\Windows\CurrentVersion\Run registry key export — ClickOnce registers persistent application shortcuts here at the user level without admin rights; malicious entries will reference .appref-ms files or point directly to the attacker-controlled update URL for silent re-execution | Email gateway SMTP message trace and attachment metadata for the 90-day lookback window — the initial .appref-ms delivery via email is the primary infection vector documented in this campaign; preserving sender IP, sending domain, attachment hash, and recipient list establishes scope of exposure and supports downstream threat intelligence sharing

Per-Action IR Details

Step 1: Containment — Audit email gateway rules immediately and add explicit block or quarantine policies for .appref-ms and .application file attachments and download links. Confirm web proxy or secure email gateway inspects ClickOnce MIME types (application/x-ms-application, application/x-ms-appref-ms). Identify any .appref-ms files delivered to mailboxes in the past 90 days using email search tools.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-4 (Information Flow Enforcement), CIS 9.2 — Use DNS Filtering Services (note: boundary control for blocking ClickOnce delivery channels where IG2/IG3 safeguards apply)

Compensating: Use PowerShell against Exchange Online or on-prem Exchange to enumerate delivered .appref-ms files: `Get-MessageTrackingLog -EventId DELIVER | Where-Object {$_.MessageSubject -match 'appref-ms'}`. For proxy inspection, configure Squid or pfSense URL filtering to block MIME types 'application/x-ms-application' and 'application/x-ms-appref-ms'. Deploy a free MXToolbox or similar header analyzer to confirm gateway enforcement is

active.

Evidence: Before modifying gateway rules, export the full 90-day email delivery log from the gateway (SMTP message trace, sender IP, recipient, attachment filename, MIME type) — this establishes the initial access vector and scope of .appref-ms delivery. Capture web proxy logs showing outbound connections to ClickOnce deployment manifests (.application URLs) — these reveal the attacker's distribution infrastructure. This step alters gateway policy state; log snapshots must be preserved before rule changes overwrite routing history.

Step 2: Detection — Query endpoint telemetry for dfsvc.exe spawning child processes (cmd.exe, powershell.exe, rundll32.exe, wscript.exe) — this process tree is anomalous outside legitimate enterprise ClickOnce deployments. Search Windows event logs and EDR for .appref-ms file execution (process creation events showing dfsvc.exe as parent). Review HKCU\Software\Microsoft\Windows\CurrentVersion\Run and user-writable startup locations for ClickOnce-registered application shortcuts. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs) to validate log coverage across endpoints.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with a config that enables Event ID 1 (Process Create) with ParentImage filtering on dfsvc.exe. Run the following PowerShell query locally or via PSRemoting across endpoints: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4688 -and $_.Message -match 'dfsvc.exe'}`. For registry persistence, run: `Get-ItemProperty 'HKCU:\Software\Microsoft\Windows\CurrentVersion\Run' | Select-Object *` on all user profiles. Use Sigma rule 'proc_creation_win_dfsvc_anomalous_child_process' (community-available) to hunt across collected Sysmon logs with a grep or chainsaw tool if no SIEM is available.

Evidence: Capture volatile state BEFORE any containment action on identified hosts: acquire full RAM image (WinPmem or Magnet RAM Capture) to preserve in-memory dfsvc.exe execution context and any injected payloads loaded by rundll32.exe. Run `Get-NetTCPConnection | Where-Object {$_.OwningProcess -eq (Get-Process dfsvc -ErrorAction SilentlyContinue).Id}` to capture live C2 connections associated with dfsvc.exe. Collect Sysmon Event ID 1 logs, Windows Security Event ID 4688 filtered on dfsvc.exe and its children, and the full contents of HKCU\Software\Microsoft\Windows\CurrentVersion\Run and %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup before any registry or file changes are made.

Step 3: Eradication — There is no vendor patch; this technique exploits intended ClickOnce behavior. Where ClickOnce is not required for business operations, disable the feature via Group Policy (Software Restriction Policies or AppLocker rules blocking dfsvc.exe execution for standard users). Remove any identified malicious .appref-ms shortcuts from user profiles and startup locations. Revoke or rotate credentials for accounts that executed suspicious ClickOnce payloads per NIST AC-2 (Account Management) and D3-CRO (Credential Rotation).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Without Group Policy infrastructure, use AppLocker in audit mode first (built into Windows 10/11 Pro and Enterprise) with a deny rule for %WINDIR%\System32\dfsvc.exe targeting standard user SIDs. Alternatively, use Software Restriction Policies (SRP) to set an Additional Rules path denial on dfsvc.exe. For credential rotation without a PAM tool, use the built-in `net user [username] [newpassword]` for local accounts and coordinate AD password resets via ADUC. Remove malicious .appref-ms files from %APPDATA%\Microsoft\Windows\Start Menu\Programs and %LOCALAPPDATA%\Apps\2.0 (ClickOnce default install path) using: `Get-ChildItem -Path $env:LOCALAPPDATA\Apps -Recurse -Filter *.appref-ms | Remove-Item -Force`.

Evidence: Before revoking credentials or disabling dfsvc.exe, preserve: (1) a full copy of %LOCALAPPDATA%\Apps\2.0\ — this is the ClickOnce application store where malicious payloads are installed at the

user level and contains the deployment manifest, executable, and update URL pointing to attacker infrastructure; (2) export HKCU\Software\Microsoft\Windows\CurrentVersion\Run as a .reg file to document persistence entries before deletion; (3) collect Windows Security Event ID 4624/4625 and 4648 logs for the compromised account covering the 90-day lookback window to assess lateral movement; (4) capture a Prefetch file for dfsvc.exe (%WINDIR%\Prefetch\DFSVC.EXE-*.pf) to establish execution history before remediation alters the filesystem.

Step 4: Recovery — After disabling or restricting ClickOnce, validate that legitimate business-critical ClickOnce applications are inventoried and explicitly allowlisted before re-enabling selectively. Monitor dfsvc.exe process activity for 30 days post-remediation. Confirm no persistent scheduled tasks or Run key entries tied to attacker-controlled update URLs remain. Apply NIST AU-12 (Audit Record Generation) controls to ensure post-remediation activity is fully logged.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-12 (Audit Record Generation), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Use `schtasks /query /fo LIST /v | findstr /i 'appref dfsvc update'` to enumerate scheduled tasks referencing ClickOnce update mechanisms on each remediated host. For Run key verification post-cleanup, re-run the HKCU\Software\Microsoft\Windows\CurrentVersion\Run query and diff against the pre-eradication export. Validate legitimate ClickOnce app inventory by cross-referencing %LOCALAPPDATA%\Apps\2.0\ manifests against a known-good software list maintained in a spreadsheet or CMDB. Enable Sysmon Event ID 1 continuous logging for dfsvc.exe with alerting via a local log forwarder (Winlogbeat + Elasticsearch free tier) for the 30-day watch period.

Evidence: Before declaring recovery complete, verify: (1) no entries remain in Task Scheduler (Event ID 4698 — Scheduled Task Created) referencing attacker-controlled update URLs embedded in ClickOnce deployment manifests; (2) %LOCALAPPDATA%\Apps\2.0\ contains only known-good application manifests with publisher certificates matching your approved software list; (3) outbound DNS and HTTP/S connections to the attacker's ClickOnce distribution server (identified from the original .application manifest file) have ceased — confirm via proxy/firewall logs covering 72 hours post-remediation. Recovery does not alter live process state on already-remediated hosts, but log continuity must be verified before closing the incident.

Step 5: Post-Incident — Conduct a gap review of email gateway rules against non-.exe delivery mechanisms (.appref-ms, .application, .lnk, .hta, .iso). Map detection coverage against T1218 (Signed Binary Proxy Execution) and T1547.001 (Registry Run Keys) in your SIEM or EDR. Reference CIS 7.1 (Vulnerability Management Process) to formalize periodic review of LOLBin and living-off-the-land technique coverage. Engage threat hunting to baseline dfsvc.exe activity across the estate using D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) to identify residual indicators.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: For teams without SIEM, use Chainsaw (free, open-source) against collected Sysmon and Windows Event logs to hunt for dfsvc.exe child process chains using the built-in Sigma rule set. Document detection gaps in a simple gap register spreadsheet mapping each ClickOnce delivery vector (.appref-ms, .application, .lnk) to whether your email gateway, AV, and endpoint logging currently detect it. Use MITRE ATT&CK Navigator (free, browser-based) to color-code T1218 and T1547.001 coverage based on your actual tool stack, producing a shareable heatmap for leadership.

Evidence: Post-incident, preserve the complete forensic package as institutional memory: (1) all collected .appref-ms files and deployment manifests from %LOCALAPPDATA%\Apps\2.0\ (hash and archive with 7-Zip AES-256); (2) the full Sysmon/Event Log export showing the dfsvc.exe → rundll32.exe process chain with timestamps; (3) the attacker's update URL extracted from the ClickOnce manifest XML (the 'deploymentProvider' element) for threat intelligence and IOC sharing; (4) the pre/post registry diff of HKCU\Software\Microsoft\Windows\CurrentVersion\Run entries. This step

does not alter live system state — no volatile capture prerequisite applies, but all evidence must be write-protected (hash-verified with sha256sum or Get-FileHash) before archival.

Detection Guidance

Primary detection pivot: dfsvc.exe spawning unexpected child processes. In any EDR or SIEM, alert on process creation where ParentImage = dfsvc.exe AND ChildImage contains cmd.exe, powershell.exe, rundll32.exe, wscript.exe, or mshta.exe. Secondary pivot: .appref-ms file execution events, filter process creation logs for command lines referencing .appref-ms extensions, particularly from user-writable paths (AppData, Temp, Downloads). Registry persistence: query for new entries under HKCU\Software\Microsoft\Windows\CurrentVersion\Run containing paths to AppData\Local\Apps (the default ClickOnce install path). Network pivot: outbound HTTP/S connections from dfsvc.exe to non-Microsoft update endpoints are anomalous; ClickOnce update calls to attacker infrastructure will appear as GET requests to .application manifest files from dfsvc.exe or its child processes. Relevant NIST controls: AU-2 (Event Logging), AU-6 (Audit Record Review), SI-4 (System Monitoring). D3FEND countermeasures: System File Analysis for startup config changes, Local Account Monitoring for account-level ClickOnce activity, System Init Config Analysis for Run key and startup folder modifications. No public IOC hashes or C2 infrastructure have been disclosed in the CrowdStrike source material; detection is behavioral, not indicator-based.

Framework Mappings

MITRE-ATTACK

- **T1566.002** — Spearphishing Link
- **T1218** — System Binary Proxy Execution
- **T1053.005** — Scheduled Task
- **T1105** — Ingress Tool Transfer
- **T1027** — Obfuscated Files or Information
- **T1547** — Boot or Logon Autostart Execution
- **T1218.011** — Rundll32
- **T1574** — Hijack Execution Flow
- **T1547.001** — Registry Run Keys / Startup Folder
- **T1204.002** — Malicious File

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CA-7** — Continuous Monitoring
- **CM-7** — Least Functionality
- **SI-7** — Software, Firmware, and Information Integrity

- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **8.2** — Collect Audit Logs

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566.002	Spearphishing Link	Initial-Access
T1218	System Binary Proxy Execution	Defense-Evasion
T1053.005	Scheduled Task	Execution
T1105	Ingress Tool Transfer	Command-And-Control
T1027	Obfuscated Files or Information	Defense-Evasion
T1547	Boot or Logon Autostart Execution	Persistence
T1218.011	Rundll32	Defense-Evasion
T1574	Hijack Execution Flow	Persistence
T1547.001	Registry Run Keys / Startup Folder	Persistence
T1204.002	Malicious File	Execution

Sources

Source	URL	Tier
Blog	https://www.crowdstrike.com/en-us/blog/new-abuse-of-the-clickonce-t...	T3
	https://www.crowdstrike.com/en-us/blog/crowdstrike-signal-transform...	T3
	https://www.crowdstrike.com/en-us/blog/av-comparatives-awards-for-e...	T3
	https://www.crowdstrike.com/en-us/blog/why-small-businesses-choose-...	T3

Source	URL	Tier
New Abuse of the ClickOnce Technology: Part 1	https://www.crowdstrike.com/en-us/blog/new-abuse-of-the-clickonce-t...	T3

Generated 2026-06-22 14:02 UTC by TJS Security Command Center